Wireless Offense & Defense for Law Enforcement
802.11 Exploitation & Tracking
we understand . . .
• . . . the technical challenges law enforcement faces while pursuing targets utilizing 802.11 technologies

• . . . and appreciate the procedural issues that are associated with these investigative techniques

• . . . we have developed a unique set of tools to address those technical challenges
We are the hammer ...
“... invincibility lies in the defense; the possibility of victory in attack ... ”

Sun Tzu
Objectives – Wi-Fi

• Market Overview
  – Public Wireless
  – Device Utilizations

• Wireless Architecture
  – Anatomy of Clients and Access Points

• Wireless Threats
  – Wireless Intelligence
  – Hidden Wireless Communications
  – Hidden Wireless Storage
  – Open Wireless

• Commercial Tools

• SR Technologies’ Tools
MARKET OVERVIEW
Where is Wi-Fi

- 10,000 Mobile hotspot locations in US alone
- 27,000 AT&T hotspots
- 104,227 US Public Locations
  - colleges, universities and public libraries
  - airports, hotels, coffee shops, etc.
  - condos and apartment buildings
  - your neighborhoods

...so these are the hosts... what about the clients
Wi-Fi Growing Trends

Worldwide location highlights: Public Wi-Fi locations

Worldwide public Wi-Fi locations: 2006 – Q2 2011

2007: 219,681
2008: 237,507
2009: 289,476
2010: 414,356
Q3 2011: 647,788

Source: JiWire, Q3 2011

Worldwide quarterly growth in public Wi-Fi locations

Q4 2010: 414,356
Q1 2011: 546,783
Q2 2011: 577,250
Q3 2011: 647,788

*Base starting at 230,000
Source: JiWire, Q3 2011
Wi-Fi Usage Globally

**Worldwide location highlights:** Public Wi-Fi locations

<table>
<thead>
<tr>
<th>Rank</th>
<th>Country</th>
<th>Q3 2011 # of Locations</th>
<th>Q2 2011 Rank</th>
<th>% Change (from Q2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>United Kingdom</td>
<td>181,474</td>
<td>1</td>
<td>26.4%</td>
</tr>
<tr>
<td>2</td>
<td>United States</td>
<td>104,277</td>
<td>3</td>
<td>8.3%</td>
</tr>
<tr>
<td>3</td>
<td>China</td>
<td>102,285</td>
<td>2</td>
<td>0.1%</td>
</tr>
<tr>
<td>4</td>
<td>South Korea</td>
<td>69,569</td>
<td>4</td>
<td>26.1%</td>
</tr>
<tr>
<td>5</td>
<td>France</td>
<td>34,600</td>
<td>5</td>
<td>12.2%</td>
</tr>
<tr>
<td>6</td>
<td>Russian Fed.</td>
<td>16,659</td>
<td>7</td>
<td>4.7%</td>
</tr>
<tr>
<td>7</td>
<td>Germany</td>
<td>14,733</td>
<td>6</td>
<td>-0.2%</td>
</tr>
<tr>
<td>8</td>
<td>Japan</td>
<td>14,685</td>
<td>9</td>
<td>17.2%</td>
</tr>
<tr>
<td>9</td>
<td>Taiwan</td>
<td>14,315</td>
<td>8</td>
<td>0.2%</td>
</tr>
<tr>
<td>10</td>
<td>Sweden</td>
<td>7,765</td>
<td>10</td>
<td>2.1%</td>
</tr>
</tbody>
</table>

**Source:** JiWire, Q3 2011

**Public Wi-Fi business models:** Worldwide Q3 2011

- Paid: 77.6%
- Free: 22.4%
- Increase in Free: 2.2%

**Public Wi-Fi business models:** U.S. Q3 2011

- Paid: 58.0%
- Free: 23.8%
- Increase in Free: 18.2%

**Source:** JiWire, Q3 2011
Device Popularity

Q3 2011

**Connected device trends: Device ownership**

*Which of the following devices do you own?*

- **Laptop**: 90% (Q2 2011), 79% (Q3 2011)
- **Smartphone**: 58% (Q2 2011), 62% (Q3 2011)
- **Tablet**: 32% (Q2 2011), 37% (Q3 2011)
- **eReader**: 16% (Q2 2011), 16% (Q3 2011)
- **Netbook**: 12% (Q2 2011), 12% (Q3 2011)

*Source: JiWire, Q3 2011*

*What do you plan to buy in the next 6 months?*

- **Tablet**: 25%
- **Smartphone**: 24%
- **Laptop**: 16%

*Source: JiWire, Q3 2011*
What is your wireless saying about you and your targets???
Wi-Fi Client Trends

• laptops consistent ~100 Million
• 100 dual mode devices
  – Wi-Fi / Cellular
  – 200 % growth annually
  – can’t get a device without Wi-Fi

Source: Skyhook Wireless & ABI Research 2007
Wi-Fi Client Trends – Cafés

• Laptops
  – 25.6% Apple Devices
  – 74.4% PC Based Devices

• Mobile Devices
  – 54% iPhone
  – 43% iTouch
  – 3% Other
Wireless to Overtake Wired

Video will be nearly 90% of Consumer IP traffic by 2012

41% CAGR 2007-2012

- Internet Video to TV
- Internet Video to PC
- VoIP
- Video Communications
- Gaming
- P2P
- Web/Data
802.11x creates significant challenges for law enforcement investigations

- create discrete, peer to peer communications anywhere quickly
- Readily available to anyone
- Easy to use, find and exploit
- Cheap - free in most cases
- Completely unsupervised, difficult to monitor
- Challenging (at best) to predict where and when
- Can not be tracked using conventional ‘Wired’ means

... so what are the consequences ...
Introduction to Wi-Fi and its components

WI-FI ARCHITECTURE
How does Wi-Fi work?

• Wi-Fi uses radio waves just like cell phone and television or more closely to a two-way radio to communicate your data.

• A network adapter translates data into a radio signal and transmits it using some sort of antenna.

• A wireless router or AP receives the signal and decodes the message, it is then either forwarded to another adapter or to the internet via a wired connection (ethernet, dsl, etc.)
Anatomy of Wi-Fi: Residential
Anatomy of Wi-Fi: Corporate
Finding Rogue Devices

• Shadow
• Direction Finding
• Survey
• Post-Analysis
Anatomy: Wi-Fi Router

Front View

Back View
Anatomy: WiFi Client

• Laptops
• Phones
  – Wi-Fi Enabled
  – Wi-Fi only
  – iPhones/iPods
• Games
  – Sony psp
  – Nintendo DS / DS lite
  – Xbox / PS3
• TV’s
• Pacemakers
• Etc…
Wireless (in)security, exploits and vulnerabilities

WIRELESS THREAT
Wireless Devices & Security

• No Physical Security
  – Access from long distance (not planned)
  – Users want access, they connect to anyone
  – Devices want access, they are pre-programmed to connect (AT&T, Sprint, Verizon)

• Paradigm shift
  – Not only protecting network
  – Educate, prevent end-user to connect to foreign networks

• Security not only when you are on
  – Rouge AP
  – Soft AP / Karmetasploit
Wireless Chatter / Rogues

- Wireless Devices Talk too much
- Pattern of Life
- Where were you ??
- Allows for Rouges
- MTM: Man in the middle
Wireless Camera’s

• Intercept Transmission
• Modify Transmission
• Distort / Interrupt Transmission

• Officer / Agent Safety
• Counter-Intelligence
• Entry Surveillance
2.4Ghz Camera
Wireless Exposure
Wireless Exposure

• Signal leakage
  – Connection signal quality
  – Sniff / Exploit signal quality

• APs Power
  – ±32mW – 400mW
  – MIMO extends the leakage

• STA Power
  – 16mW – 75mW
Child Porn / Wireless Implications


- Sometimes we get lucky

---

**Post details: D.Ore.: Keeping child pornography on a wireless network accessible to anyone showed no REP**

**02/03/10**

Defendant’s computer was set to share files on his wireless network. A neighbor’s wireless router failed, and her computer, which regularly shared files, too, automatically picked up defendant’s system, and she saw folders indicative of child pornography. The defendant had no reasonable expectation of privacy in the files that could be shared by anybody who accessed his wireless network. United States v. Ahmadi, 2010 U.S. Dist. LEXIS 7621 (D. Ore. January 28, 2010):

A. *Diminished Reasonable Expectation of Privacy in Data Broadcast via Unsecured Wireless Network Router*

At the suppression hearing, defendant argued that a wireless network should be given no less protection than a hardwired network under the Fourth Amendment. According to defendant, if, hypothetically, defendant had possessed a hardwired home network, and officer McCullough had obtained access to defendant’s computer via the hardwired network, there would no question that his access violated a reasonable expectation of privacy.
Gatekeeper

• Leave behind device
• Save resources
• Announces arrival of target
• MAC Address
• Keyword
  – GUID
  – GNUTELLA
  – EMAIL
Identity / Child Exploitations

• Open Access Points – Public Locations

• Identity is Hidden

• “On the internet no one knows you’re a dog”

• Wireless crime, wireless criminals: *Investigating 802.11 networks and the people who abuse them* by Christa Miller - 7/2009
HIDDEN COMMUNICATIONS
Dynamic ‘Hidden’ Communication

- ‘Hidden’ in plan sight
- Uncommon Devices
- 802.11 Wireless Phones
- Readily Available
- Game Systems
  - Nintendo DS
  - Sony PSP
Kids & Technology

- iTouch
- PSP
- DS Lite
Scenario: Commercial Flight

• Observation of flight from California → Georgia
• WiFi Spectrum ch 11
• Open WiFi Clients
• ‘Free Public WiFi’ Virus
  – Viral ... Virus ???
  – No Free WiFi
MiFi

- MiFi – or Mobile WiFi – is a new kind of mobile broadband modem that lets you share your mobile broadband connection with several WiFi enabled devices such as laptops, games consoles, iPod Touch or digital cameras.
Wireless Storage

• DLink Photo Frame
• AirStach
• Apple Time Capsule
What is being used today?

COMMERCIAL WIRELESS TOOLS

SRT Wireless, LLC. Proprietary and Confidential Information
WiFi Exploit Tools

- Kismet
- AirCrack-NG
- #Inssider
- WiFi Fo Fum
- Yellow Jacket
- Cardinal / Shadow
Kismet

- Wireshark/Tcpdump compatible data logging
- Airsnort compatible weak-iv packet logging
- Network IP range detection
- Built-in channel hopping and multicard split channel hopping
- Hidden network SSID decloaking
- Manufacturer and model identification of access points and clients
- Runtime decoding of WEP packets for known networks
Aircrack-NG

- **Aircrack-ng** is a network detector / client detector
- Packet Sniffer
- WEP and WPA Cracker
- Analysis tool for 802.11 WLAN’s
- It works with any wireless card whose driver supports raw monitor mode (Prism II or Atheros most common)
- can sniff 802.11a / b / g traffic
- The program runs under Linux and Windows
- Linux is the preferred and easier to implement
Aircrack-NG

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aircrack-ng</td>
<td>Cracks WEP (Brute-force search) and WPA (Dictionary File) keys.</td>
</tr>
<tr>
<td>airdecap-ng</td>
<td>Decrypts WEP or WPA encrypted capture files with known key.</td>
</tr>
<tr>
<td>airmon-ng</td>
<td>Placing different cards in monitor mode.</td>
</tr>
<tr>
<td>aireplay-ng</td>
<td>Packet injector (Linux, and Windows [with Commview drivers]).</td>
</tr>
<tr>
<td>airodump-ng</td>
<td>Packet sniffer: Places air traffic into PCAP or IVS files and shows information about networks.</td>
</tr>
<tr>
<td>airtun-ng</td>
<td>Virtual tunnel interface creator.</td>
</tr>
<tr>
<td>airolib-ng</td>
<td>Stores and manages ESSID and password lists; Increases the KPS of WPA attacks</td>
</tr>
<tr>
<td>packetforge-ng</td>
<td>Create encrypted packets for injection.</td>
</tr>
<tr>
<td>Tools</td>
<td>Tools to merge and convert.</td>
</tr>
</tbody>
</table>

Aircrack-ng 0.6

<table>
<thead>
<tr>
<th>CH</th>
<th>PWR</th>
<th>ESSID</th>
<th>Beacon</th>
<th># Data</th>
<th>CH</th>
<th>NB</th>
<th>ENC</th>
<th>ESSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:03:09:43:22:44</td>
<td>100</td>
<td>55</td>
<td>0</td>
<td>10</td>
<td>54</td>
<td>WEP</td>
<td>wendao_300B</td>
<td></td>
</tr>
<tr>
<td>00:0F:B5:50:38:EA</td>
<td>130</td>
<td>60</td>
<td>139</td>
<td>10</td>
<td>54</td>
<td>WEP</td>
<td>Geek-Debian</td>
<td></td>
</tr>
</tbody>
</table>

Key found! [OC:FC:28:33:43]
#insidder - metageek

- Network Stumbler
- Lists AP
- No Stations
- Easy to use

http://www.metageek.net/docs/inssider-user-guide
Backtrack v4

- LINUX Distro
- Kismet
- AIRCRACK-NG
- Promiscuous / RF Mon
Cardinal/ Shadow

- Multi-Channel
- LE Modes
- Tactical Solution
- Active / Passive Modes